IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Okunseinde et al.**	§	Group Art Unit: **2437**
	§	
Serial No. **10/803,590**	§	Examiner: **Gergiso, Techane**
	§	
Filed: **March 18, 2004**	§	Customer No.: **50170**
	§	
For: **Providing Transaction-Level Security**	§	
	§	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

APPELLANTS' BRIEF (37 C.F.R. § 41.37)

This Appeal Brief is in furtherance of the Notice of Appeal filed February 9, 2010 (37 C.F.R. § 41.31).

The fees required under § 41.20(b)(2), and any required petition for extension of time for filing this brief and fees therefore, are dealt with in the accompanying Fee Transmittal.

I. Real Party in Interest

The real party in interest in this appeal is the following party: International Business Machines Corporation of Armonk, New York.

II. Related Appeals and Interferences

With respect to other appeals and interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

III. Status of Claims

The status of the claims involved in this proceeding is as follows:

1. Claims canceled: 9-27 and 30
2. Claims withdrawing from consideration but not canceled: NONE
3. Claims pending: 1-8, 28-29, and 31-34
4. Claims allowed: NONE
5. Claims rejected: 1-8, 28-29, and 31-34

The claims on appeal are: claims 1-8, 28-29, and 31-34.

IV. Status of Amendments

Appellants filed an After Final Amendment on February 9, 2010 in which clarifying amendments were made to the claims. In an Advisory Action mailed February 22, 2010, the Examiner erroneously stated that the amendments raised new issues requiring further search and consideration. Appellants respectfully submit that none of the amendments made in the After Final Amendment raise any new issues that would require further consideration and/or search. Thus, the Examiner's refusal to enter the February 9, 2010 After Final Amendment was improper.

V. Summary of Claimed Subject Matter

With regard to independent claim 1, a method is provided that comprises determining security information associated with a object **(e.g., BO 130 in Figure 1)** of a transaction **(e.g., page 12, lines 13-14; page 13, lines 5-8)**. The security information is inserted in a header **(e.g., 220, 240 in Figure 2; page 16, lines 1-2, 8-9)** of the object and the object is to be transmitted from a source device **(e.g., 110(1) in Figure 1)** to a target device **(e.g., 110(5) in Figure 1; page 19, lines 10-13)** along a transmission path **(e.g., page 20, lines 17-21; dotted line in Figure 4; page 25, lines 19-22)** that includes at least one intermediate device **(e.g., 110(2-4) in Figure 1)**. The method further comprises determining, at each of the source device **(e.g., 110(1) in Figure 1)**, and the at least one intermediate device **(e.g., 110(2-4) in Figure 1)** along the transmission path **(e.g., dotted line in Figure 4; page 25, lines 19-22)** as the object is transmitted along the transmission path **(e.g., dotted line in Figure 4; page 25, lines 19-22)**, whether a next device in the transmission path to which the object is to be transmitted provides a level of security indicated by at least a portion of the security information in the header **(e.g., 220 in Figure 2; 320 in Figure 3; page 17, lines 16-22; page 20, lines 7-13; page 21, lines 4-21; page 28, line 20 to page 29, line 10)** of the object **(e.g., page 13, lines 8-11)**. The method further comprises transmitting, at each of the source device, and the at least one intermediate device along the transmission path as the object is transmitted along the transmission path **(e.g., page 24, lines 1-16; page 25, lines 17-19; dotted line in Figure 4; page 25, lines 19-22)**, the object to the next device in the transmission path in response to determining that the next device provides the level

of security required by the at least a portion of the security information **(e.g., 350 in Figure 3; page 23, lines 9-15)**.

Regarding claim 28, a method is provided that comprises receiving, at a first device **(e.g., 110(3) in Figure 1)** along a transmission path **(e.g., page 20, lines 17-21; dotted line in Figure 4; page 25, lines 19-22)** from a source device **(e.g., 110(1) in Figure 1)** to a target device **(e.g., 110(5) in Figure 1; page 19, lines 10-13)**, a request from a second device **(e.g., 110(1) or 110(2) in Figure 1; 325 in Figure 3; page 21, lines 16-17)** along the transmission path **(e.g., page 20, lines 17-21; dotted line in Figure 4; page 25, lines 19-22)** desiring to transmit an object to a third device **(e.g., 110(5) in Figure 1)**. The request includes at least a portion of security information associated with the object **(e.g., 220, 240 in Figure 2; page 16, lines 1-2, 8-9)**, the portion of security information being provided in a header of the object **(e.g., 220, 240 in Figure 2; page 16, lines 1-2, 8-9)**. The method further comprises determining if the first device is adapted to provide a level of security identified by the at least a portion of security information in the header of the object **(e.g., 220 in Figure 2; 320 in Figure 3; page 17, lines 16-22; page 20, lines 7-13; page 21, lines 4-21; page 28, line 20 to page 29, line 10)**. Moreover, the method comprises transmitting an indication to the second device, based on determining if the first device provides the level of security identified by the at least a portion of security information **(e.g., 330 in Figure 3; page 22, lines 10-11)**. In addition, the method comprises receiving, in the first device, the object from the second device only in response to the first device transmitting an indication that the first device provides the level of security identified by the at least a portion of security information **(e.g., 350 page 23,lines 9-15)**.

VI. Grounds of Rejection to be Reviewed on Appeal

The grounds of rejection to be reviewed on appeal are as follows:

(1) the rejection of claims 1, 3, and 5 under 35 U.S.C. § 112, second paragraph as being allegedly indefinite; and

(2) the rejection of claims 1-2, 4, 6-8, 28-29, and 31-34 under 35 U.S.C. § 103(a) as being

allegedly unpatentable over Suzuki (U.S. Patent Application Publication No. 2004/00259529) in view of Lee, IV et al. (U.S. Patent Application Publication No. 2005/0188072).

VII. Argument

A. Rejection under 35 U.S.C. § 112, Second Paragraph

The Final Office Action rejects claims 1, 3, and 5 under 35 U.S.C. § 112, second paragraph as being allegedly indefinite. This rejection is respectfully traversed.

With regard to claim 1, the Final Office Action alleges that because the claim recites at least three devices, i.e. a source device, an intermediate device, and a target device to form the path, that somehow this invalidates the recitation of "a next device in the transmission path" and renders the claim indefinite. Appellants respectfully disagree.

Simply reciting at least 3 devices does not invalidate a recitation of a "next device." If one is transmitting from a first device to a second device, then the second device is the "next device" along the path. Thus, for example, if the transmission is going from the source device to the intermediate device, then the intermediate device is the "next device" along the path. Similarly, if the intermediate device is transmitting to a target device, then the target device is the "next device" along the path. The phrase "next device" along the path is specifically used in the claims because there may actually be more than one intermediate device and thus, it is possible that the "next device" is not a single intermediate device or the target device, but can be a second, third, fourth, etc., intermediate device. All that is required is that a determination is made as to whether a "next device" in the transmission path, be that any one of the one or more intermediate devices or the target device, to which the object is to be transmitted, provides a level of security indicated by at least a portion of the security information in the header of the object. Thus, the recitation of the phrase "a next device in the transmission path" does not render the claim indefinite.

Regarding claim 3, it is Appellants' understanding that the Final Office Action alleges that the claim does not recite a plurality of alternatives from which "at least one of" the alternatives is performed. In the After Final Amendment filed February 9, 2010, Appellants attempted to amend claim 3 to clarify the alternatives for the Examiner by replacing the term

"and" with "or." However, the Examiner refused entry of this amendment alleging that it raised new issues requiring further search and consideration. Regardless, Appellants respectfully submit that the claim is clear even with the term "and" being in the claim because it is clear that the alternatives are (1) transmitting information representative of the level of security that is desired to the next device in the transmission path prompts the next device in the transmission path to execute at least one module that allows the next device in the transmission path to provide the level of security; and (2) comparing the next device in the transmission path to a list of trusted devices in the header portion of the object, since the claim recites "at least one of:" and includes these two alternatives within indention and with the conjunction "and" meaning it is one element selected from the set comprising (1) and (2) above.

Accordingly, Appellants respectfully submit that claim 3 clearly recites the alternatives corresponding to the phrase "at least one of:". In view of the above, Appellants respectfully request that the Board overturn the rejection of claims 1, 3, and 5 under 35 U.S.C. § 112, second paragraph.

B. Rejection under 35 U.S.C. § 103(a)

The Final Office Action rejects claims 1-2, 4, 6-8, 28-29, and 31-34 under 35 U.S.C. § 103(a) as being allegedly unpatentable over Suzuki (U.S. Patent Application Publication No. 2004/0259529) in view of Lee, IV et al. (U.S. Patent Application Publication No. 2005/0188072). This rejection is respectfully traversed.

1. Independent Claims 1 and 28

Independent claim 1 reads as follows:

1. A method, comprising:
determining security information associated with a object of a transaction, wherein the security information is inserted in a header of the object and the object is to be transmitted from a source device to a target device along a transmission path that includes at least one intermediate device;
determining, at each of the source device, and the at least one intermediate device along the transmission path as the object is transmitted

along the transmission path, whether a next device in the transmission path to which the object is to be transmitted provides a level of security indicated by at least a portion of the security information in the header of the object; and

transmitting, at each of the source device, and the at least one intermediate device along the transmission path as the object is transmitted along the transmission path, the object to the next device in the transmission path in response to determining that the next device provides the level of security required by the at least a portion of the security information.
(emphasis added)

Appellants respectfully submit that neither Suzuki nor Lee, either alone or in combination, teach or render obvious at least the features of claim 1 emphasized above.

Suzuki is directed to a wireless adhoc communication system in which frame transmission source authentication is performed among terminals involved in delivery of the frames. Specifically, a first terminal generates a keyed hash value by using an authentication header key determined with respect to a second terminal and gives it to an authentication header of a frame. The second terminal generates a keyed hashed value by using the authentication header key determined with respect to the first terminal and compares it with the authentication header given to the frame. If the keyed hashed value generated at the second terminal matches the authentication header it is confirmed that the frame ***has been transmitted from the first authenticated valid terminal.*** The first terminal encrypts a payload part by using a unicast encryption key determined with respect to a third terminal. This encrypted payload part can be decrypted only by the third terminal having the unicast encryption key (see Abstract of Suzuki).

Thus, essentially Suzuki is directed to validating that a frame is being sent from an authenticated valid terminal. Suzuki is not concerned with determining whether a next device along a transmission path provides a level of security indicated by at least a portion of the security information in the header of an object being transmitted. To the contrary, Suzuki is specifically looking backward to the source to determine if the source was valid. At no time in the operation of the wireless adhoc communication system of Suzuki is there any determination as to whether the next target of the transmission provides a required level of security as specified in a header of the frame prior to transmitting the object to the next target.

Moreover, nowhere in Suzuki is there any teaching or technical rationale provided for transmitting an object along the transmission path to the next device ***in response to determining***

that the next device provides a level of security required by the portion of the security information in the header of the object. To the contrary, in Suzuki, the frame is processed only when it is determined that the ***source*** of the frame, i.e. the terminal from which the frame is transmit, is an authenticated valid terminal. Suzuki is not concerned with whether the next device to which the frame is being transmitted provides a required level of security as specified in a header of the frame.

The Final Office Action points to paragraphs [0011], [0021], [0044], [0050], and [0073]-[0074] of Suzuki as teaching these features (Final Office Action, pages 4-5). These paragraphs of Suzuki read as follows (emphasis added):

> [0011] In one form of the terminal of the present invention, the terminal may further include: a path table having at least one path list for holding a transfer destination terminal identifier for causing a frame to arrive at another terminal in such a manner as to correspond to the terminal identifier of the other terminal; and means for searching the path table for the path list containing an end-point terminal identifier and transmitting the frame to the transfer destination terminal identifier when the authentication header is valid and the end-point terminal identifier of the frame is not the terminal identifier of the other terminal and for discarding the frame when the authentication header is not valid. As a result, an operational effect is obtained such that, ***when the fact that the authentication header given to the received frame is generated by a valid transmission terminal is confirmed, the frame is transferred to the next transfer destination terminal, and if the authentication header is not valid, the frame is discarded.***
>
> [0021] In another aspect, the present invention provides an encryption method for use in a terminal having a key management list table having at least one key management list for holding authentication header keys with respect to other terminals in such a manner as to correspond to the terminal identifiers of the other terminals, the encryption method including the steps of: searching the key management list table for the key management list containing the reception terminal identifier of a frame to be transmitted in order to extract the corresponding authentication header key; generating a keyed hashed value, in which the extracted authentication header key is hashed together with a predetermined area of the frame, and giving the keyed hashed value as an authentication header to the frame; and transmitting the frame. As a result, an operational effect is obtained such that the reception terminal is made to confirm that a valid authentication header is given on the basis of the keyed hash function, whose strength is ensured.

[0044] The terminal B receiving the frame confirms whether or not the authentication header 809 is valid by using the authentication header key (AHK_AB) with respect to the terminal A. When it is confirmed that the authentication header 809 is valid, the terminal B generates an authentication header 809 by using an authentication header key (AHK_BC) with respect to the terminal C which is the next transmission source and gives the authentication header to the frame. In that case, the encrypted payload part 802 is transmitted as is. On the other hand, if the authentication header 809 is not valid, the frame is discarded without being delivered to the next transmission source.

[0050] The authentication header 809 is authentication data used to perform frame transmission source authentication. An authentication header key (AHK) is determined in advance between the transmission terminal and the reception terminal. Then, in the transmission terminal, a keyed hashed value, in which a predetermined area of a transmission frame and the authentication header key are hashed together, is generated, and this hashed value is given as the authentication header 809. In the reception terminal, a keyed hashed value, in which a predetermined area of a reception frame and the authentication header key are hashed together, is generated, and this hashed value is compared with the authentication header 809. If the result of this comparison shows a match, it is confirmed that the received frame has been transmitted from the transmission frame.

[0073] Furthermore, the terminal A generates the authentication header key (AHK_AB) (133). The authentication header key is generated randomly or on the basis of a random number in the manner described above. This authentication header key should be changed as appropriate. The terminal A encrypts the generated authentication header key (AHK_AB) in accordance with the public key (PK_B) of the terminal B, and transmits it as an authentication header key distribution message 1342 to the terminal B (134). The terminal B receiving the authentication header key distribution message 1342 decrypts the authentication header key in accordance with the secret key of the terminal B itself (234).

[0074] The terminal A and the terminal B set the authentication header key (AHK_AB) obtained in this manner in the key management list table 670 (FIG. 6) of its own terminal (135, 235). That is, the terminal A sets the authentication header key (AHK_AB) in the column of the authentication header key 673 of the key management list having the terminal B as the terminal identifier 671. The terminal B sets the authentication header key (AHK_AB) in the column of the authentication header key 673 of the key management list having the terminal A as the terminal identifier 671. In this manner, the terminals which form the wireless adhoc communication system share the authentication header key with respect to the adjacent terminal.

Paragraph [0011] merely teaches a path list and that the frame is only transmitted when the ***source*** of the frame is authenticated; otherwise it is discarded. The citation of paragraph [0011] only serves to bolster Appellants' position that Suzuki teaches authenticating the ***source*** of a frame, not determining whether ***a next device along the path provides a required security level as specified in a header of an object that is to be transmitted.***

Paragraph [0021] merely teaches a key management table for terminals and using the keys in the key management table to get the key for the terminal to which the frame is to be transmitted and hashing a piece of the frame with the key and then transmitting the frame. While this paragraph mentions getting a key for a terminal to which the frame is being transmitted, this paragraph does not make any mention of determining whether a next device along a transmission path provides a level of security indicated by at least a portion of the security information in the header of the frame. To the contrary, the encryption using the key is merely a way of authenticating that the frame came from an authorized valid terminal.

Paragraph [0044] merely teaches an example in which terminal B confirms that the authentication header of a frame is valid using an authentication header key with respect to terminal A (from which the frame was sent). If it is confirmed, then terminal B generates an authentication header for terminal C and transmits the frame with the new authentication header to terminal C. Again, this is merely to authenticate that the frame is being ***sent from*** an authorized valid terminal, i.e. the header generated by terminal B would be invalid if terminal B did not already know the key for terminal C.

Paragraph [0050] merely teaches that the key is determined ahead of time between the source and the target of the transmission and that this key is used by the target to generate an encrypted portion of a frame that can then be compared against the encryption value in the header to determine if the frame ***is coming from an authenticated valid terminal***. Again, this is merely teaching a mechanism for authenticating ***the source*** of a frame, not determining whether a next device along a transmission path provides a required level of security as specified by security information in a header of an object being transmitted.

Paragraphs [0073]-[0074] merely describes a flowchart outlining the operation discussed above with regard to using a key to generate a hashed value that can be compared against a value in a header of a frame to determine if the frame ***is coming from an authenticated valid source***.

Thus, it is clear from the above that the cited portions of the Suzuki reference, in actuality, do not teach or render obvious the specific features of claim 1 as emphasized above but instead only serve to further support Appellants' position that Suzuki teaches authentication a source rather than ensuring that a next device along a transmission path provides a required level of security.

The Final Office Action admits that Suzuki does not teach security information that is associated with a transaction object or providing a level of security indicated by at least a portion of the security information (see Final Office Action, page 5). However, the Final Office Action alleges that these features are taught by Lee. Appellants respectfully disagree.

Lee is directed to a mechanism for dynamically constructing a protocol to facilitate communication between nodes and across multiple nodes. Policies associated with the nodes are used to specify protocol properties of the nodes. A policy expression in a policy related to a node can be selected by another node to construct a protocol between the two nodes. A policy expression selection process can be applied to multiple nodes in a communication path to construct a protocol across the multiple nodes (see paragraph [0007]). A computer can retrieve an intermediate node policy characterizing communication properties supported by the intermediate node and may request destination node policies characterizing communication properties supported by a destination node (paragraphs [0009]-[0010]).

With Lee, the protocol must be established first before any actual message communications are performed between a source and a destination. Lee provides a mechanism for establishing such a protocol dynamically based on the policies of the nodes between the source and destination. Essentially, the mechanism of Lee creates a protocol that is supported by all of the nodes along a communication path prior to performing any communication. This essentially means that the protocol that is created has a minimum number of protocol properties according to the lowest common denominator amongst the nodes.

Lee does not provide any teaching, or technical rationale, to implement the features of providing security information in a header of an object of a transaction, at least a portion of the security information identifying a required level of security required for each device along a transmission pathway, or using the portion of the security information at each device along the transmission pathway to determine if a next device along the pathway provides the required level of security and transmitting the object to the next device if the next device provides the required level of security. To the contrary, Lee is concerned with connection level protocol establishment,

rather than providing a transaction level security mechanism, as is recited in claim 1. Lee is not concerned with performing security level checks on each individual device of a transmission path, whether the individual device provides a level of security required by header information an object of a transaction prior to the object being transmitted to the device and transmitting the object to that device in response to a determination that the device supports the required level of security. In fact, with Lee there is no need to perform a check at each device along a transmission path as to whether a next device along the transmission path provides a required level of security since the protocol is established a priori before any transmission is performed.

The Final Office Action points to paragraph [0028], [0043], [0054], [0094], and [0106] to [0107] of Lee as allegedly teaching security information associated with a transaction object providing a level of security. These portions of Lee are reproduced below (emphasis added):

> [0028] To further illustrate the concept of a policy, a policy can specify message encoding formats, security algorithms, tokens, transport addresses, transaction semantics, routing requirements, and other properties related to message transmission or reception. Implementations of policies described herein specify one or more assertions, which can aid two or more nodes in a message exchange in determining if their requirements and capabilities are compatible. The assertions may be grouped and related to each other in some way. A group of one or more assertions may be referred to as a policy expression.
>
> [0043] The exemplary policy 200 includes two policy expressions bounded by a <wsp: ExactlyOne> operator 202. A first policy expression 204 expresses a security profile (i.e., <wsse:SecurityToken>) consisting of security specific policy assertions. As shown in FIG. 2, the first policy expression 204 specifies "Kerberos Authentication" (i.e., <wsse: TokenType>wsse: Kerberosv5TGT </wsse:TokenType>-) and "Privacy" (i.e., <wssx: Privacy/>).
>
> [0054] It will be appreciated that by using a policy, such as policy 200, a node can specify capabilities, requirements, the number of messages and their form, ***security measures***, reliable messaging, transactions, routing, and other parameters relevant to a message exchange. In addition, policies are extensible, whereby a policy can be extended to include, for example, newly available policy expressions.
>
> [0094] Thus, the policy-compliant message 512 that is sent from the source node 502, may be viewed as a message with three levels of policy application. The policy-compliant message 512 includes an inner level of policy application 514 that relates to the destination node 504 and will be received and validated last in

the message exchange. The policy-compliant message 512 includes a middle level of policy application 516 related to the intermediate node Y 508 and will be received and validated next-to-last in order. The policy-compliant message 512 includes an outer level of policy application 518 related to the intermediate node X 508 and will be received and validated first in the message exchange.

[0106] The selected policy expressions associated with each node in the node sequence will be applied to the message in order of farthest to closest. A creating operation 616 creates a new message by applying the selected policy expression corresponding to the next farthest node (starting with the farthest node) on the node list to a message to be sent to the destination node. The first time the creating operation 616 executes, the first selected policy expression is applied to an underlying message; subsequent executions of the creating operation 616 apply another selected policy expression to the previously created message. Thus, the creating operation 616, when iteratively executed, generates a message with one or more levels of policy applied to the message.

[0107] A determining operation 618 determines whether all the policies corresponding to all the nodes in the node list have been applied. If not all the policies have been applied, the operation 600 branches 'NO' to the creating operation 616, which applies another level of policy corresponding to the next node on the node list.

These sections of Lee mention building up a message based on policies of the nodes in a path where the policies can specify the security measures of the node. However, there is no mention or even technical rationale provided anywhere in these, or any other, sections of Lee regarding the specific features of claim 1 with regard to determining, ***at each of the source device, and the at least one intermediate device along the transmission path as the object is transmitted along the transmission path***, whether ***a next device in the transmission path*** to which the object is to be transmitted ***provides a level of security indicated by at least a portion of the security information in the header of the object***. Moreover, there is no teaching or technical rationale provided in these, or any other, sections of Lee regarding the specific features of transmitting, ***at each of the source device, and the at least one intermediate device along the transmission path as the object is transmitted along the transmission path***, the object to the next device in the transmission path ***in response to determining that the next device provides the level of security required by the at least a portion of the security information***

In summary, the Suzuki reference uses keys and hash values to authenticate that data is being transmitted from a valid ***source***. Suzuki does not teach checking the next device to which

the data is to be transmitted to see if the next device provides a required level of security as specified in the header of the data to be transmitted. Thus, Suzuki essentially looks backwards to see if the data is coming from a valid source whereas the claimed invention looks forward to see if the next device provides the required level of security before transmitting the data. Thus, Suzuki does not teach or render obvious the features of the claimed invention. Moreover, the Lee reference also does not teach or render obvious these features as discussed above. Hence, any alleged combination of Suzuki and Lee, even if such a combination were possible and one were somehow motivated to attempt such a combination, *arguendo*, would still not result in the features of independent claim 1 being taught or rendered obvious.

These distinctions, likewise, apply to similar features in independent claim 28. That is, independent claim 28 specifically recites determining if the first device ***provides a level of security identified by the at least a portion of security information in the header of the object***; transmitting an indication to the second device, based on determining if the first device provides the level of security identified by the at least a portion of security information; and receiving, in the first device, the object from the second device ***only in response to the first device transmitting an indication that the first device provides the level of security identified by the at least a portion of security information***. As noted above, neither Suzuki nor Lee, either alone or in combination, teach or render obvious such features.

In view of the above, Appellants respectfully submit that the alleged combination of Suzuki and Lee fails to teach or render obvious at least those features of independent claim 1 or the similar features in independent claim 28. At least by virtue of their dependency on claims 1 and 28, respectively, Suzuki and Lee fail to teach or render obvious the features of dependent claims 2, 4, 6-8, 29, and 31-34. Accordingly, Appellants respectfully request that the Board of Patent Appeals and Interferences overturn the rejection of claims 1-2, 4, 6-8, 28-29, and 31-34 under 35 U.S.C. § 103(a).

2. Dependent Claims 2-8, 29, and 31-34

In addition, dependent claims 2-8, 29, and 31-34 recite additional features that are not taught or rendered obvious by the alleged combination of Suzuki and Lee.

a. Claim 2

For example, with regard to claim 2, the alleged combination of references fails to teach transmitting to the next device in the transmission path information representative of the level of security that is desired or receiving a response from the next device in the transmission path indicating that the next device in the transmission path provides the desired level of security. The Final Office Action alleges that these features are taught by Lee at paragraphs [0011], [0034], and [0037] which read as follows:

> [0011] In yet another implementation, a system includes a source node policy having protocol parameters related to a source node and a policy retriever retrieving an intermediate node policy having protocol parameters related to and intermediate node between the source node and a destination node in a communication path. The system also includes a message generator generating a request message in accordance with the intermediate node policy, the request message including a request for a destination node policy having protocol parameters related to the destination node.
>
> [0034] The policy retriever 134 retrieves policies from other nodes, such as node B 104 or intermediate nodes on the network 106. The policy retriever 134 can request a policy from another node, receive the policy, and may cache a received policy in memory for later use. The policy retriever 134 can also retrieve a policy that was previously stored in local memory on node A 102. The policy retriever 134 also performs functions related to determining whether a retrieved policy is compatible with a local policy and/or selecting a compatible policy expression in a retrieved policy.
>
> [0037] The policy retriever 140 at node B 104 has functionality similar to the functionality described above with respect to policy retriever 134 at node A 102. The message generator 142 at node B 104 formats and transmits messages to node A 102 in accordance with one or more assertions in the input policy 108 of node A 102.

Paragraph [0011] merely teaches that the system includes a source node policy, a policy retriever for retrieving an intermediate node policy, and a message generator that generates a request message. Paragraph [0034] merely teaches that the policy retriever retrieves policies from other nodes by requesting the policy from another node, receiving the policy, and caching the received policy or retrieving the policy from local memory. The retriever can also determine if the retrieved policy is compatible with a local policy and select a compatible policy expression in the

retrieved policy. Paragraph [0037] merely teaches that node B's policy retriever operates in the same way as the policy retriever of node A and has a message generator that transmits a message in accordance with an input policy of node A.

While these sections of Lee talk about policy retrieval for intermediate nodes, nothing in these sections, or any other sections, of Lee mention or render obvious the specific features of transmitting to the next device in the transmission path information representative of the level of security that is desired or receiving a response from the next device in the transmission path indicating that the next device in the transmission path provides the desired level of security. To the contrary, Lee retrieves the policy for the intermediate node and determines compatible expressions in the intermediate node's policy that are compatible with the policy of the source node. Lee does not transmit information to the intermediate node information representative of a level of security that is desired. Moreover, Lee does not receive a response indicating that the next device in the transmission path provides the desired level of security. Thus, neither Suzuki nor Lee, either alone or in combination, teach or render obvious these specific features of claim 2.

b. Claim 6

As a further example, regarding claim 6, the alleged combination of Suzuki and Lee fails to teach or render obvious the features of determining an alternative device along a different transmission path that provides the level of security required by the at least a portion of the security information in response to determining that the next device in the transmission path does not provide the level of security required by the at least a portion of the security information. The Final Office Action alleges that these features are taught by Lee at paragraphs [0083]-[0088] and [0100].

Paragraphs [0083]-[0088] read as follows (emphasis added):

> [0083] The operations described above pertain to environments in which one node is communicating with another node using dynamic protocol construction. Often, in actual operation, messages from one node are routed through other nodes before reaching the destination node. For example, in a corporate environment, messages may be routed through a firewall, a main server, and finally to a recipient's computer. Each node in the path may have policies related to data protocols that are preferred, available, and/or required by the node.

[0084] FIG. 5 illustrates an exemplary multiple node communication environment 500 including a source node 502 and a destination node 504. A message exchange occurs between the source node 502 and the destination node 504, via two intermediate nodes, intermediate node X 506, and intermediate node Y 508. Source node 502, destination node 504, intermediate node X 506, and intermediate node Y 508 each have a policy. The policy at each node can include one or more policies (e.g., input policy, output policy), as discussed above. ***In general, the source node 502 retrieves policies in order from closest node to farthest node, and applies policies to a message in order from farthest node to closest node, as is illustrated by an exemplary scenario below.***

[0085] Source node 502 generates a message intended for the destination node 504. As discussed above, source node 502 retrieves the policy of the destination node 504, in order to select a policy expression, and apply the selected policy expression to the message. However, in order to retrieve the policy of the destination node 504, the source node 502 must go through intermediate node X 506 and intermediate node Y 508.

[0086] In the exemplary scenario described with respect to the environment 500, it is assumed that source node 502 initially has no information about (i.e., is not aware of) the presence of intermediate node Y 508, but is aware of intermediate node X 506. ***In order to retrieve the policy from destination node 504, the source node 502 first requests the policy from intermediate node 506. The source node 502 selects a policy expression from the policy related to intermediate node X 506 and applies the selected policy expression to a policy retrieval message.***

[0087] The policy retrieval message is a request for the policy from the destination node 504. Included with the policy retrieval message is the policy related to the source node 502. The intermediate node X 506 receives the policy retrieval message, including the policy of the source node 502, and validates the message, as discussed above, by checking to see that a valid policy expression was applied to the policy retrieval message. If the policy retrieval message is valid, the intermediate node X 506 requests the policy from the destination node 504.

[0088] ***The intermediate node X 506 puts the policy of the destination node 504 into a message for the source node 502. This includes applying the policy of the source node 502 to the message so that the message to the source node 502 conforms to the policy of the source node 502. The source node 502 receives and validates the message and reads the policy of the destination node 504.***

Paragraphs [0083]-[0088] describe a process of getting the destination node policy by obtaining policy from an intermediate node, selecting a policy expression from the policy of the intermediate node and applying it to a policy retrieval message that includes the policy for the source node. The intermediate node receives the policy retrieval message, validates it based on the valid selected policy expression that was applied to the policy retrieval message, and then requests the policy from the destination node. The intermediate node then places the policy of the destination node into a message for the source node by applying a policy of the source node to the message and sending it back to the source node. Thus, the policies are used to authenticate the source of policy information.

Nothing in these sections teaches or renders obvious the specific features of determining an alternative device along a different transmission path that provides the level of security required by the at least a portion of the security information in response to determining that the next device in the transmission path does not provide the level of security required by the at least a portion of the security information. There is not even the mention of an alternative device anywhere in any of these paragraphs. Thus, contrary to the allegations raised in the Office Action, these sections of Lee do not in fact teach or render obvious the specific features of claim 6.

With regard to paragraph [0100], Lee is stating that the mechanism of Lee determines if a node requires routing to another node, i.e. a routing assertion. This does not teach anything about determining an alternative device along a different transmission path ***that provides the level of security required*** by the at least a portion of the security information ***if the next device does not support the level of security required.*** All that Lee is stating here is that if a node specifies another node to which it must route communications, Lee identifies that node. Neither Suzuki nor Lee, either alone or in combination, teach or render obvious these specific features of claim 6.

c. Claims 7 and 29

Regarding claim 7 (and claim 29), the alleged combination of references fails to teach or render obvious the specific feature of sending a message to the next device in the transmission path instructing the next device to execute at least one module that allows the next device to

provide the level of security required by at least a portion of the security information. The Final Office Action again points to paragraphs [0083]-[0088] of Lee as allegedly teaching this feature. However, as shown above, these paragraphs only describe retrieving a destination policy by retrieving an intermediate node policy, selecting a compatible expression from the policy to authenticate a request for the destination policy, sending the request to the intermediate node which authenticates the request based on the compatible expression and requests the policy from the destination node. The intermediate node then sends a message back to the source using a compatible expression selected from the source policy, the message including the destination node policy. Nowhere in this process is there any mention of sending a message to a next device instructing that device to execute a module that allows the next device to provide a level of security required by the at least a portion of the security information, as recited in claim 7 (and claim 29). Neither Suzuki nor Lee, either alone or in combination, teach or render obvious these specific features of claims 7 and 29.

d. Claim 31

With regard to claim 31, this claim recites a specific implementation of the method of claim 1 in which there are two intermediate nodes and the method is first implemented at the source node with regard to the first intermediate node being the "next node" in the transmission path and then the method is performed at the first intermediate node (which then operates as the "source node") with regard to a second intermediate node (which then operates as the "next node" in the transmission path). Just as with claim 1 above, the alleged combination of Suzuki and Lee fails to teach or render obvious the features of claim 31.

The Final Office Action points to many different sections of Lee as allegedly teaching the specific features of claim 31 but none of these paragraphs or Figures actually teach any of these features (see Final Office Action, page 31). In fact, it is unclear what the Examiner's position is since many of these features, which are specific applications of the methodology of claim 1 to specific nodes, i.e. source, first intermediate, second intermediate, and target nodes, which were alleged to be taught by Suzuki are now instead alleged as being taught by Lee. This seems contradictory and is evidence of the weakness of the Examiner's position with regard to the present claims allegedly reading on the features of the references. It is unclear what the Examiner believes is equivalent to these features since the Examiner takes two different positions

with regard to the same references. Regardless, for similar reason6s as set forth above, Appellants respectfully submit that neither Suzuki nor Lee, either alone or in combination, teach or render obvious the specific features of claim 31 at least for similar reasons as specified above with regard to claim 1.

In particular, the Final Office Action points to paragraphs [0010], [0021], [0083]-[0088], [0094], [0104], [0108], and Figure 5, element 500 as allegedly teaching the features of claim 31. Paragraphs [0083]-[0088] of Lee are addressed above with regard to claim 6 and are shown to only teach retrieving a destination policy by retrieving an intermediate node policy, selecting a compatible expression from the policy to authenticate a request for the destination policy, sending the request to the intermediate node which authenticates the request based on the compatible expression and requests the policy from the destination node. Paragraph [0094] is addressed above with regard to claim 1 and is shown to only teach a three layer policy application message having layers corresponding to a destination node and intermediate nodes. None of these paragraphs teach or render obvious the specific features of claim 31.

Paragraphs [0010], [0031], [0104], and [0108] of Lee read as follows:

> [0010] In another implementation, a method includes retrieving an intermediate node policy and a destination node policy, the intermediate node policy characterizing communication properties supported by an intermediate node and the destination node policy characterizing communication properties supported by a destination node, the intermediate node being between a source node and the destination node in a communication path. The method further includes applying the intermediate node policy and the destination node policy to an underlying message in order of the destination node policy followed by the intermediate node policy.
>
> [0031] Expression (1) indicates that in order to comply with the A input policy 108, a node attempting to send a message to node A can satisfy either assertion A1, assertion A2, and assertion A3 together, or assertion A4, assertion A5, and assertion A6 together, but typically not both groups of assertions. The manner in which a node, such as node B 104, may use the A input policy 108 to communicate with node A 102 is discussed further below. Other, non-Boolean, expressions can be used to express relationships among assertions.
>
> [0104] The retrieving operation 604 then sends the created policy request to the first node in the list. The first node in the list removes a policy level (related to the first node) from the message and forwards the request message on to the next node. The next node receives the policy request message and, if the request is for

the node's policy, that node sends back its policy. Otherwise, the request is forwarded on to the next node.

[0108] If all of the selected policy expressions have been applied, the operation 600 branches `YES` to a transmitting operation 620. The transmitting operation 620 transmits the finally created message, having all levels of policy applied. Each of the levels of policy is removed upon receipt by the node corresponding to that level of policy, and the message is sent on to the next node in the communication path, until the message reaches the destination node.

Other than merely mentioning source, intermediate, and destination nodes, these paragraphs have nothing to do with the specific features of claim 31. That is, none of these paragraphs teach, or even provide any technical rationale to implement, the features of (1) determining if a next device in the transmission path provides a level of security required by the at least a portion of security information including performing the determining at the source device, wherein the next device is the first intermediate device; (2) transmitting the object to the next device comprising transmitting the object to the first intermediate device; or (3) in response to determining that the next device provides the level of security, and in response to determining that the first intermediate device provides the level of security: determining, at the first device, if a second device of the plurality of intermediate devices that is adjacent the first device provides the level of security indicated by the at least a portion of the security information; transmitting the object to the second device of the plurality of intermediate devices in response to determining that the second device provides the level of security; and transmitting the object to the target device from the second device. None of these features are taught or rendered obvious by the cited portions, or any other portion, of the Lee reference, whether taken alone or in combination with the Suzuki reference.

Figure 5 of Lee is shown in the Evidence Appendix where element 500 refers to all of the elements shown in Figure 5. Figure 5 shows a plurality of nodes including a source node, intermediate nodes, and a destination node, all having associated policies, and the build up of policies in a message as shown in elements 512-518. What is not shown in Figure 5 is any of the specific features of claim 31 discussed above. Appellants agree that Lee teaches a source node, a plurality of intermediate nodes, and a destination node and the build up of a message based on policies from these nodes. However, this is not what is recited in claim 31. Neither Suzuki nor Lee, either alone or in combination, teach or render obvious these specific features of claim 31.

e. Claim 32

Regarding claim 32, this claim recites similar features to claim 6 discussed above. However, instead of citing paragraphs [0083]-[0088] and [0100] as in the rejection of claim 6, the Examiner instead cites paragraphs [0054] and [0100] in the rejection of claim 32 (see Final Office Action, page 8). Paragraph [0100] has been addressed above with regard to the rejection of claim 6. Paragraph [0054] of Lee merely teaches that a policy allows a node to specify capabilities, requirements, the number of messages and their form, security measures, reliable messaging, transactions, routing, and other parameters relevant to a message exchange. Stating that a policy allows a node to specify capabilities, requirements, etc. does not teach or render obvious the feature of ***determining an alternative intermediate device along a different transmission path that provides a level of security represented in response to determined that at least one of the first intermediate device and the second intermediate device in the transmission path does not provide the level of security***, as recited in claim 32. Neither Suzuki nor Lee, either alone or in combination, teach or render obvious these specific features of claim 32.

f. Claim 33

With regard to claim 33, the alleged combination of Suzuki and Lee fails to teach or render obvious the features of determining if a next device in the transmission path provides a level of security comprises determining, at a previous device in the transmission path, a security level for each intermediate device of the plurality of intermediate devices. Moreover, the alleged combination fails to teach or render obvious the features of transmitting the object to the next device in the transmission path, in response to determining that the next device provides the level of security, comprises transmitting the object to each of the plurality of intermediate devices in the transmission path in response to determining that each of the plurality of intermediate devices provides the level of security.

The Final Office Action points to paragraphs [0084], [0094], and [0100] of Lee as allegedly teaching all of these features. Paragraph [0100] is reproduced above. Paragraphs [0084] and [0094] read as follows:

[0084] FIG. 5 illustrates an exemplary multiple node communication environment 500 including a source node 502 and a destination node 504. A message exchange occurs between the source node 502 and the destination node 504, via two intermediate nodes, intermediate node X 506, and intermediate node Y 508. Source node 502, destination node 504, intermediate node X 506, and intermediate node Y 508 each have a policy. The policy at each node can include one or more policies (e.g., input policy, output policy), as discussed above. ***In general, the source node 502 retrieves policies in order from closest node to farthest node, and applies policies to a message in order from farthest node to closest node, as is illustrated by an exemplary scenario below.***

[0094] Thus, the policy-compliant message 512 that is sent from the source node 502, may be viewed as a message with three levels of policy application. ***The policy-compliant message 512 includes an inner level of policy application 514 that relates to the destination node 504 and will be received and validated last in the message exchange. The policy-compliant message 512 includes a middle level of policy application 516 related to the intermediate node Y 508 and will be received and validated next-to-last in order. The policy-compliant message 512 includes an outer level of policy application 518 related to the intermediate node X 508 and will be received and validated first in the message exchange.***

While these paragraphs teach that the message includes multiple layers of policies that are retrieved from the nodes along a path to a destination node, there still is no teaching in any of these sections regarding determining, at a previous device in the transmission path, ***a security level for each intermediate device of the plurality of intermediate devices***. Moreover, there is no teaching of transmitting the object to each of the plurality of intermediate devices in the transmission path ***in response to determining that each of the plurality of intermediate devices provides the level of security***. All that Lee teaches is that the policies of the nodes are gathered and applied to a message in a layered manner. This does not teach or render obvious the specific features of claim 33. Neither Suzuki nor Lee, either alone or in combination, teach or render obvious these specific features of claim 33.

g. Claim 34

Regarding claim 34, the alleged combination fails to teach or render obvious the features of the object being one of a plurality of objects of the transaction, and wherein at least two of the objects in the plurality of objects have different security information in their respective headers identifying different levels of security required to be provided by devices along corresponding

transmission paths to receive the at least two objects. The Final Office Action again points to paragraphs [0083]-[0088] and [0100] of Lee as allegedly teaching these features. These paragraphs are addressed and reproduced above. It is plainly evident from the above that there is not even the mention of objects, let alone multiple objects of a transaction or at least two objects of the same transaction having different levels of security required by devices along the transmission path. There simply is no correlation between what is described in the cited paragraphs and the features of claim 34. Neither Suzuki nor Lee, either alone or in combination, teach or render obvious these specific features of claim 34.

VIII. Conclusion

In view of the above, Appellants respectfully submit that claims 1-8, 28-29, and 31-34 of the present application are directed to statutory subject matter and that the features of these claims are not taught or suggested by the Suzuki or Lee references. Accordingly, Appellants request that the Board of Patent Appeals and Interferences overturn the rejections set forth in the Final Office Action.

Respectfully submitted,

Stephen J. Walder, Jr.
Reg. No. 41,534
Walder Intellectual Property Law, P.C.
17330 Preston Road, Suite 100B
Dallas, TX 75252
(972) 380-9475
ATTORNEY FOR APPELLANTS

CLAIMS APPENDIX

1. A method, comprising:

determining security information associated with a object of a transaction, wherein the security information is inserted in a header of the object and the object is to be transmitted from a source device to a target device along a transmission path that includes at least one intermediate device;

determining, at each of the source device, and the at least one intermediate device along the transmission path as the object is transmitted along the transmission path, whether a next device in the transmission path to which the object is to be transmitted provides a level of security indicated by at least a portion of the security information in the header of the object; and

transmitting, at each of the source device, and the at least one intermediate device along the transmission path as the object is transmitted along the transmission path, the object to the next device in the transmission path in response to determining that the next device provides the level of security required by the at least a portion of the security information.

2. The method of claim 1, wherein the object is a business object, and wherein determining if the next device in the transmission path provides the level of security comprises:

transmitting to the next device in the transmission path information representative of the level of security that is desired; and

receiving a response from the next device in the transmission path indicating that the next device in the transmission path provides the desired level of security.

3. The method of claim 1, wherein determining the security information comprises accessing the header portion of the object;

wherein determining if the next device in the transmission path provides a level of security indicated comprises performing at least one of:

transmitting information representative of the level of security that is desired to the next device in the transmission path prompts the next device in the transmission path to execute at least one module that allows the next device in the transmission path to provide the level of security; and

comparing the next device in the transmission path to a list of trusted devices in the header portion of the object;

wherein the transmitting the object to the next device in the transmission path comprises transmitting the object to an object handler module in the next device in the transmission path;

wherein the object handler module is a business integration adapter supporting connectivity options, the connectivity options comprising at least one of packaged applications, custom applications, legacy applications, databases, trading partners' systems, and public information stores on the internet;

wherein the object handler module supports at least one of event-driven real-time synchronous connections, asynchronous loosely coupled connections with trading partners, synchronous on-demand connections to customers and synchronous tightly coupled connections to trusted trading partners;

wherein the object handler module includes at least one of a module for accessing the security information associated with a given object and a module for requesting the adjacent intermediate device in the transmission path to provide information about its security

capabilities.

4. The method of claim 1, wherein determining the security information comprises determining security information relating to at least one of connection information, class information, trusted entities information, and logging capability information.

5. The method of claim 3, wherein accessing the header portion of the object comprises accessing at least one header of a Simple Object Access Protocol message.

6. The method of claim 1, further comprising determining an alternative device along a different transmission path that provides the level of security required by the at least a portion of the security information in response to determining that the next device in the transmission path does not provide the level of security required by the at least a portion of the security information.

7. The method of claim 1, further comprising sending a message to the next device in the transmission path instructing the next device to execute at least one module that allows the next device to provide the level of security required by the at least a portion of the security information.

8. The method of claim 1, wherein determining the security information comprises determining the security information in response to receiving the object from at least one of a previous device or a source device in the transmission path.

28. A method, comprising:

receiving, at a first device along a transmission path from a source device to a target device, a request from a second device along the transmission path desiring to transmit an object to a third device, wherein the request includes at least a portion of security information associated with the object, the portion of security information being provided in a header of the object;

determining if the first device is adapted to provide a level of security identified by the at least a portion of security information in the header of the object; and

transmitting an indication to the second device, based on determining if the first device provides the level of security identified by the at least a portion of security information; and

receiving, in the first device, the object from the second device only in response to the first device transmitting an indication that the first device provides the level of security identified by the at least a portion of security information.

29. The method of claim 28, further comprising configuring the first device with at least one module that provides the level of security.

31. The method of claim 1, wherein at least one intermediate device includes at least a first intermediate device and a second intermediate device;

wherein determining if a next device in the transmission path provides a level of security required by the at least a portion of security information includes performing the determining at the source device, wherein the next device is the first intermediate device;

wherein transmitting the object to the next device comprises transmitting the object to the

first intermediate device, and wherein in response to determining that the next device provides the level of security, and in response to determining that the first intermediate device provides the level of security:

determining, at the first device, if a second device of the plurality of intermediate devices that is adjacent the first device provides the level of security indicated by the at least a portion of the security information;

transmitting the object to the second device of the plurality of intermediate devices in response to determining that the second device provides the level of security; and

transmitting the object to the target device from the second device.

32. The method of claim 31, further comprising determining an alternative intermediate device along a different transmission path that provides the level of security represented in response to determining that at least one of the first intermediate device and the second intermediate device in the transmission path does not provide the level of security.

33. The method of claim 1, wherein the at least one intermediate device includes a plurality of intermediate devices;

wherein determining if a next device in the transmission path provides a level of security comprises determining, at a previous device in the transmission path, a security level for each intermediate device of the plurality of intermediate devices;

wherein transmitting the object to the next device in the transmission path, in response to determining that the next device is adapted to provide the level of security, comprises

transmitting the object to each of the plurality of intermediate devices in the transmission path in response to determining that each of the plurality of intermediate devices provides the level of security;

further comprising:

transmitting the object to the target device.

34. The method of claim 1, wherein the object is one of a plurality of objects of the transaction, and wherein at least two of the objects in the plurality of objects have different security information in their respective headers identifying different levels of security required to be provided by devices along corresponding transmission paths to receive the at least two objects.

EVIDENCE APPENDIX

Figure 5 of Lee (U.S. Patent Application Publication No. 2005/0188072):

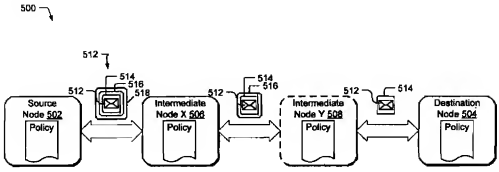

Fig. 5

RELATED PROCEEDINGS APPENDIX

NONE